Finanse, Rynki Finansowe, Ubezpieczenia nr 6/2016 (84), cz. 1

DOI: 10.18276/frfu.2016.84/1-23 s. 269–279

Rola i zadania audytu bezpieczeństwa systemów informatycznych na przykładzie jednostki sektora administracji rządowej

Sebastian Bartoszewicz, **Anna Batoszewicz***

Streszczenie: *Cel* – Celem artykułu jest przedstawienie roli i zadań audytu bezpieczeństwa systemów informatycznych w jednostkach sektora finansów publicznych oraz wskazanie zagrożeń funkcjonowania tychże systemów.
Metodologia badania – Aby zrealizować cel artykułu, wykorzystano analizę literatury przedmiotu badań i aktów prawnych w przedmiotowym zakresie. W części empirycznej przedstawiono studium przypadku przeprowadzania audytu bezpieczeństwa systemów informatycznych w wybranym podmiocie publicznym. Wnioskowanie przeprowadzono metodą indukcji.
Wynik – W artykule zaprezentowano aspekt teoretyczny audytu bezpieczeństwa systemów informatycznych i przedstawiono praktyczne podejście do tego zagadnienia, opierając się na przebiegu ww. procesu w wybranej jednostce sektora administracji rządowej.
Oryginalność/wartość – W opracowaniu dokonano analizy zadań audytu bezpieczeństwa systemów informatycznych oraz zidentyfikowano zagrożenia związane z funkcjonowaniem tych systemów.

Słowa kluczowe: audyt wewnętrzny, audyt bezpieczeństwa systemów informatycznych, audyt informatyczny, jednostki sektora administracji rządowej

Wprowadzenie

Ogromne tempo rozwoju technologicznego spowodowało, że jednostki sektora finansów publicznych pracują obecnie przy użyciu specjalistycznych systemów informatycznych. Chcąc spełnić oczekiwania społeczeństwa informacyjnego, wiele urzędów zinformatyzowało swoje struktury, umożliwiając tym samym zrealizowanie spraw przy użyciu odpowiednich aplikacji i systemów informatycznych. Informacja elektroniczna stała się jednym z kluczowych elementów funkcjonowania jednostek, a poszczególne podmioty w coraz większym stopniu uzależniły swoją działalność od systemów informatycznych i danych w nich zawartych.

* mgr Sebastian Bartoszewicz (CGAP), Urząd Kontroli Skarbowej w Olsztynie, Oddział Audytu Środków Pochodzących z Budżetu Unii Europejskiej oraz Innych Źródeł Zagranicznych, 10-408 Olsztyn, ul. Lubelska 37, e-mail: s.bartoszewicz@uks.olsztyn.pl; dr Anna Bartoszewicz, Uniwersytet Warmińsko-Mazurski w Olsztynie, Wydział Nauk Ekonomicznych, Katedra Rachunkowości, 10-719 Olsztyn, ul. Oczapowskiego 4, e-mail: anna.bartoszewicz@uwm.edu.pl.

Obecnie każda jednostka publiczna zbiera, przetwarza i przechowuje zbiory danych w systemach elektronicznych. Mając na uwadze fakt, iż w dzisiejszych czasach prawie każdy obywatel ma dostęp do sieci informatycznej, powyższe dane powinny być w odpowiedni sposób chronione. Istnieje bowiem potencjalne zagrożenie ich utraty lub kradzieży.

Jak podkreślają A. Nowak i W. Scheffs (2010, s. 22), w dobie cyfryzacji rodzą się nowe przestępstwa wykorzystujące komputer jako narzędzie, które dokonane w wyniku włamań komputerowych, złośliwymi kodami i wirusami, szpiegostwem, sabotażem czy też wandalizmem, doprowadzić mogą do utraty ważnych informacji. Z tego względu utrzymanie i doskonalenie bezpieczeństwa informacyjnego staje się nieodzowne w funkcjonowaniu każdej jednostki, zwłaszcza publicznej.

Zdaniem J. Łuczaka utrata informacji staje się zjawiskiem coraz bardziej powszechnym i trudnym do wykrycia. Ponadto niewiele jest sytuacji kryzysowych mających miejsce w firmach, które można porównać do tego zjawiska. Niesie to bowiem ze sobą nie tylko konsekwencje prawne i finansowe, ale również utratę wiarygodności podmiotu, który dopuszcza osoby trzecie do swoich danych (Łuczak, 2004, s. 10–11).

Przeciwdziałając powyższym zagrożeniom, kierownictwo jednostek coraz częściej korzysta z instrumentu ochrony danych elektronicznych – audytu bezpieczeństwa systemów informatycznych. Pozwala to z jednej strony na identyfikację zagrożeń w ich funkcjonowaniu, z drugiej zaś daje możliwość wdrożenia pewnych mechanizmów, które będą niwelować zagrożenia w przyszłości. Celem artykułu jest przedstawienie roli i zadań audytu bezpieczeństwa systemów informatycznych w jednostkach sektora finansów publicznych oraz wskazanie zagrożeń funkcjonowania tychże systemów.

1. Teoretyczno-prawne aspekty audytu bezpieczeństwa systemów informatycznych

Audyt bezpieczeństwa systemów informatycznych jest zagadnieniem trudnym do jednoznacznego zdefiniowania. Punktem wyjścia do interpretacji tego pojęcia jest audyt informatyczny, który został określony przez organizację ISACA (Information Systems Audit and Control Association) jako „proces gromadzenia i oceniania dowodów w celu określenia, czy systemy informatyczne i związane z nimi zasoby: właściwie chronią majątek, utrzymują integralność danych i systemu, dostarczają odpowiednich i rzetelnych informacji, efektywnie osiągają cele organizacji, oszczędnie wykorzystują zasoby, czy w praktyce istnieją mechanizmy kontroli wewnętrznej, które zapewniają, że są osiągane cele operacyjne i kontrolne oraz że zapobiega się występowaniu niepożądanych zdarzeń lub są one na czas wykrywane, a ich skutki korygowane" (Molski, Łacheta, 2007, s. 4).

Jak wskazuje treść powyższej definicji, audyt informatyczny jest zagadnieniem bardzo obszernym, dotyczącym wielu aspektów organizacji i obejmuje wszystkie procesy oraz zasoby wchodzące w skład środowiska informatycznego. Do najważniejszych zalicza się weryfikację stanu bezpieczeństwa systemów informatycznych oraz w razie potrzeby

pojedynczych aplikacji z perspektywy występującego ryzyka oraz zaimplementowanych procedur kontrolnych. Zatem audyt bezpieczeństwa systemów informatycznych będzie jego składową.

Bezpieczeństwo powyższych systemów w dużej mierze uzależnione jest od zagrożeń, które mogą wystąpić w jednostce, dlatego istotne staje się określenie ich źródeł. K. Liderman (2012, s. 155) wskazuje w tym zakresie: siły natury (pożar, powódź, huragan, trzęsienie ziemi, epidemie), błędy ludzi i ich działania (niewłaściwe wykorzystanie lub celowe działanie na szkodę jednostki), awarie sprzętu komputerowego, awarie oprogramowania, awarie infrastruktury usługowej (zasilanie, klimatyzacja, woda, ogrzewanie). Natomiast A. Żebrowski i W. Kwiatkowski (2000, s. 73) zwracają uwagę, iż zagrożenie bezpieczeństwa informacyjnego może nastąpić na skutek działania człowieka, który dopuszcza się wykorzystania określonych technik włamań do systemów informacyjnych będących cennym źródłem informacji stanowiących tajemnicę państwową lub służbową.

Człowiek jest inicjatorem działań powodujących utratę informacji, a jego poczynania mogą być wynikiem dwóch rodzajów przesłanek. Pierwsze dotyczą działań zamierzonych, kiedy z premedytacją dokonuje on czynności negatywnie wpływających na jednostkę, lub też przypadkowe, gdy z powodu braku wiedzy w danej dziedzinie niewłaściwie wykorzystuje zasoby. Z tego względu ważne jest, aby w każdej jednostce wdrożyć mechanizmy, które pozwolą na bieżące monitorowanie i aktualizowanie systemów informatycznych oraz będą zapobiegać potencjalnym zagrożeniom. Audytorzy w tej materii mają ważną rolę do spełnienia, bowiem ich zadaniem jest wydanie opinii na temat bezpieczeństwa systemów informatycznych, wskazanie obszarów ryzyka w tym zakresie oraz zalecenie kierunków ewentualnej poprawy.

W Polsce wraz z wejściem w życie ustawy z 27 sierpnia 2009 roku o finansach publicznych w treści art. 68 ust. 2 zwrócono uwagę na bezpieczeństwo systemów informatycznych. Jako jeden z celów kontroli zarządczej wymieniono ochronę zasobów, co oznacza konieczność sprawdzenia mechanizmów zabezpieczających te zasoby. W celu otrzymania zapewnienia w tym zakresie kierownictwo jednostki powinno zlecić audytorom przeprowadzanie corocznego audytu wewnętrznego w zakresie bezpieczeństwa systemu informatycznego.

Zdaniem A. Gałacha (2005, s. 5) wdrożenie i utrzymywanie efektywnych zasad zarządzania bezpieczeństwem systemu informatycznego jest jednym z podstawowych elementów zapewnienia ochrony informacji przetwarzanych we współczesnej organizacji. 31 maja 2012 roku weszło w życie Rozporządzenie (2012). Wprowadziło ono liczne wymagania w przedmiotowym zakresie, między innymi zobowiązało większość jednostek administracji rządowej do realizowania corocznych wewnętrznych audytów bezpieczeństwa swojej infrastruktury informatycznej lub uczestniczenia w szkoleniach z obszaru bezpieczeństwa. Ponadto narzuciło wymagania, które muszą być spełnione dla nowych systemów, a istniejącym zaleciło wdrożyć mechanizmy ochronne przy pierwszej dużej modyfikacji.

Wprowadzenie obowiązku przeprowadzania audytu bezpieczeństwa systemów informatycznych wywołało wiele spekulacji na temat umiejętności i wiedzy audytorów w tym zakresie. Zrodziły się pytania dotyczące formy i sposobu realizacji samego audytu, dlatego wprowadzono standardy i wytyczne w zakresie jego przeprowadzania.

2. Wybrane wytyczne, normy i standardy w zakresie audytu bezpieczeństwa systemów informatycznych

W celu zarysowania ram i przekazania wskazówek odnośnie do sposobu przeprowadzania audytów bezpieczeństwa systemów informatycznych w jednostkach sektora finansów publicznych Ministerstwo Finansów opracowało dokument *Wspólne stanowisko Departamentu Informatyzacji Ministerstwa Administracji i Cyfryzacji oraz Departamentu Audytu Sektora Finansów Publicznych Ministerstwa Finansów odnośnie zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji* oraz *Wytyczne dotyczące prowadzenia audytu bezpieczeństwa informacji przez komórkę audytu Wewnętrznego.*

Wytyczne w przedmiotowym zakresie zostały także zawarte w Polskiej Normie PN-ISO/IEC 27001. Zgodnie z brzmieniem § 20 ust. 3 Rozporządzenia (2012) jeżeli system zarządzania bezpieczeństwem został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie polskich norm związanych z tą normą, wymagania określone w § 20 ust. 1 i 2 Rozporządzenia (2012) uznaje się za spełnione. Zapisy te potwierdzają, że Polska Norma PN-ISO/IEC 27001 może stanowić punkt odniesienia przy prowadzeniu audytów bezpieczeństwa. Opracowana została przez Polski Komitet Normalizacyjny i wyznacza standardy służące zarządzaniu bezpieczeństwem informacji. Oparta jest na międzynarodowej normie ISO/IEC 27001, która określa wymagania dla ustanowienia, wdrożenia, zarządzania, monitorowania i przeglądu udokumentowanego systemu zarządzania bezpieczeństwem informacji (SZBI) w organizacji. Zawiera kompletną listę celów kontrolnych i zabezpieczeń dla ochrony informacji, a w załączniku do niej przedstawiono normatywny wykaz wymagań zabezpieczenia, które podzielone zostały na 11 następujących obszarów:

- polityka bezpieczeństwa,
- organizacja bezpieczeństwa informacji,
- zarządzanie aktywami,
- bezpieczeństwo zasobów ludzkich,
- bezpieczeństwo fizyczne i środowiskowe,
- zarządzanie systemami i sieciami,
- kontrola dostępu,
- pozyskiwanie, rozwój i utrzymanie systemów informatycznych,
- zarządzanie incydentami związanymi z bezpieczeństwem informacji,
- zarządzanie ciągłością działania,
- zgodność z przepisami prawa.

Dużą zaletą Normy jest kompleksowe podejście do bezpieczeństwa informacji, bowiem poruszono w niej obszary bezpieczeństwa zarówno fizycznego, jak i osobowego, teleinformatycznego oraz prawnego. I chociaż nie określa ona szczegółowych wymagań technicznych, to wskazuje na płaszczyzny, które należy uregulować. Sposób zabezpieczenia tych obszarów zależy od kierowników jednostek i powinien być oparty na przeprowadzonej analizie ryzyka. Ze względu na kompleksowe podejście do tematu bezpieczeństwa informacji oraz

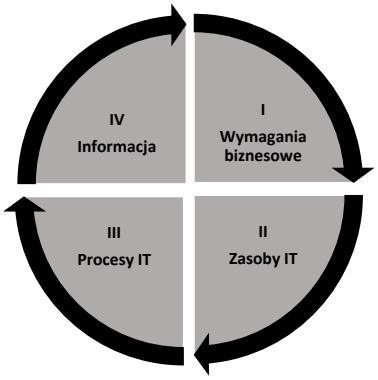
ogólny charakter wymagań Norma może być podstawą do budowy systemu zarządzania bezpieczeństwem informacji (SZBI) w organizacjach oraz stanowić punkt odniesienia dla oceny istniejącego systemu. Należy także wspomnieć, iż Polska Norma PN-ISO/IEC 27001 zaleca stosowanie modelu: „planuj – wykonuj – sprawdzaj – działaj" (PDCA), który jest wykorzystywany do całej struktury procesów SZBI. Proces wdrażania SZBI zilustrowano na rysunku 1.

Rysunek 1. Model Deminga stosowany w procesach SZBI – cykl PDCA
Źródło: opracowanie własne na podstawie PN-ISO/IEC 27001:2007.

Od 2014 roku obowiązuje Polska Norma PN-ISO/IEC 27001:2014-12, która zaktualizowała i zastąpiła normę z 2007 roku.

Ramy postępowania przy audycie bezpieczeństwa systemów informatycznych opisano również międzynarodowym standardem COBIT, który został opracowany przez stowarzyszenie ISACA (Information Systems Audit and Control Association) oraz IT Governance Institute. Stanowi on zestaw dobrych praktyk dla audytorów wykonujących przedmiotowy audyt, a metodyka COBIT służy jako pomoc w zarządzaniu, kontroli i audycie systemów informatycznych. Informacja stanowi podstawę w COBIT. Na jej podstawie organizacja diagnozuje swoje potrzeby dotyczące systemów informatycznych, które przyczynią się do osiągnięcia i realizacji celów. Mapę zależności COBIT zilustrowano na rysunku 2.

Jak wskazano na rysunku 2, wymagania biznesowe (I) inicjują zasoby IT (II) organizacji, te zaś wykorzystywane są przez procesy IT (III) służące dostarczeniu informacji (IV), która ostatecznie odpowiada za wymagania biznesowe. Z kolei każde wymaganie biznesowe jest opisane przez 7 zasad informacyjnych, które stanowią jednocześnie kryteria kontrolne pozwalające zweryfikować stopień spełnienia wymagania. Należą do nich: skuteczność, wydajność, poufność, integralność, dostępność, zgodność, wiarygodność.



Rysunek 2. Mapa zależności COBIT
Źródło: opracowanie własne na podstawie Board Briefing on IT Governance (2003).

COBIT koncentruje się na procesach, dzieląc obszar IT na 4 domeny: planowanie i organizacja, zakupy i wdrożenia, dostarczanie i wspieranie oraz monitorowanie i ocena, do których przypisane są 34 procesy. Dla każdego procesu w COBIT zdefiniowano punkty kontrolne, dla których osoba przeprowadzająca ocenę musi znaleźć uzasadnione potwierdzenie ich spełnienia w ramach ocenianej organizacji. W obszarze zasobów IT wyróżniono 4 elementy: aplikacje, informację, infrastrukturę i ludzi. Metodyka COBIT stworzona została z myślą o jej wykorzystaniu w kompleksowym audycie systemów informatycznych. Istnieje jednak możliwość ograniczenia prac audytowych wyłącznie do audytu bezpieczeństwa systemów informatycznych. W tym celu należy ograniczyć analizę tylko do procesów ocenianych według wybranych kryteriów, na przykład poufności, integralności i dostępności, oraz kryteriów pierwszorzędnych.

Audytorzy wewnętrzni zatrudnieni w jednostkach sektora finansów publicznych w swoich corocznych planach powinni ujmować zadania związane z bezpieczeństwem informatycznym, dzięki czemu kierownicy audytowanych podmiotów będą posiadali informację na temat aktualnego stanu bezpieczeństwa informatycznego jednostek. Należy podkreślić, że taki audyt umożliwi kierownikom podjęcie odpowiednich działań mających na celu wyeliminowanie luk wpływających na bezpieczeństwo systemów oraz umożliwi diagnozę braków w dokumentacji lub zasobach organizacji.

3. Audyt bezpieczeństwa informatycznego w jednostce administracji rządowej – studium przypadku

Na potrzeby realizacji celu artykułu posłużono się przykładem funkcjonowania audytu bezpieczeństwa systemów informatycznych w jednostce administracji rządowej. W wyniku przeprowadzonej analizy dokumentacji źródłowej ustalono, iż badanie audytowe w przedmiotowym zakresie przebiegało w 5 etapach (rys. 3).

Rysunek 3. Etapy procesu audytu bezpieczeństwa systemów informatycznych w podmiocie badań.

Źródło: opracowanie własne.

Pierwszy etap audytu bezpieczeństwa systemów informatycznych w podmiocie badań polegał na wskazaniu obszarów przewidzianych do audytu. Jak wynika z przeprowadzonej analizy, audytorzy wymienili 7, które należało poddać ocenie:

Obszar I: Zarządzanie aktywami.
Obszar II: Kontrola dostępu.
Obszar III: Kryptografia.
Obszar IV: Bezpieczeństwo fizyczne i środowiskowe.
Obszar V: Bezpieczna eksploatacja.
Obszar VI: Bezpieczeństwo komunikacji.
Obszar VII: Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych.

Wyznaczenie powyższych obszarów było punktem wyjścia do etapu drugiego, który oparty był na identyfikacji potencjalnych rodzajów ryzyka dla każdego z nich. Audytorzy, opierając się na analizie aktów prawnych oraz dokumentacji jednostki odnoszącej się do wskazanych obszarów, opracowali potencjalne rodzaje ryzyka, które zagrażały bezpieczeństwu systemów informatycznych w podmiocie badań. Dane w przedmiotowym zakresie przedstawiono w tabeli 1.

Tabela 1

Zidentyfikowane rodzaje ryzyka w podmiocie badań

Obszar	Rodzaje ryzyka
1	2
I. Zarządzanie aktywami	1. Ryzyko niezidentyfikowania wszystkich aktywów jednostki i niezdefiniowania właściwej odpowiedzialności w zakresie sprawowania nad nimi ochrony 2. Ryzyko niezapewnienia odpowiedniego poziomu ochrony informacji zgodnie z ich poziomem ważności dla jednostki 3. Ryzyko nieuprawnionego ujawnienia, modyfikacji, usunięcia lub zniszczenia informacji zapisanych na nośnikach
II. Kontrola dostępu	1. Ryzyko braku ograniczeń w dostępie do informacji i środków przetwarzania informacji 2. Ryzyko niezapewnienia właściwego dostępu do informacji uprawnionym użytkownikom 3. Ryzyko, że dostęp do systemów i usług będą mieli nieuprawnieni użytkownicy 4. Ryzyko niezapewnienia możliwości rozliczalności dostępu użytkowników 5. Ryzyko, że w jednostce nie wdrożono odpowiednich mechanizmów, aby zapobiec nieuprawnionemu dostępowi do systemów i aplikacji

1	2
III. Kryptografia	1. Ryzyko niezapewnienia właściwego i skutecznego wykorzystania kryptografii do ochrony poufności informacji
IV. Bezpieczeństwo fizyczne i środowiskowe	1. Ryzyko, że w jednostce nie wdrożono odpowiednich mechanizmów, aby zapobiec nieuprawnionemu fizycznemu dostępowi, kradzieży lub zniszczeniu nośników informacji i środków ich przetwarzania należących do jednostki 2. Ryzyko, że w jednostce nie wdrożono odpowiednich mechanizmów, aby zapobiec zniszczeniu, uszkodzeniu, kradzieży lub utracie integralności aktywów oraz zakłóceniom w działaniu jednostki
V. Bezpieczna eksploatacja	1. Ryzyko niezapewnienia w jednostce poprawnej i bezpiecznej eksploatacji środków przetwarzania informacji 2. Ryzyko niezapewnienia informacjom i środkom przetwarzania informacji ochrony przed szkodliwym oprogramowaniem 3. Ryzyko niezapewnienia w jednostce ochrony przed utratą danych 4. Ryzyko, że w jednostce zdarzenia nie są rejterowane i nie jest zbierany materiał dowodowy 5. Ryzyko niezapewnienia integralności systemów produkcyjnych 6. Ryzyko, że w jednostce nie wdrożono mechanizmów, aby zapobiec wykorzystywaniu podatności technicznych
VI. Bezpieczeństwo komunikacji	1. Ryzyko, że nie zapewniono ochrony informacji w sieciach oraz wspomagających je środkach przetwarzania informacji 2. Ryzyko braku zachowania bezpieczeństwa informacji przesyłanych wewnątrz jednostki i wymienianych z podmiotami zewnętrznymi
VII. Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych	1. Ryzyko niezapewnienia odpowiedniego bezpieczeństwa informacji jako nieodłącznej części systemów informacyjnych 2. Ryzyko niezapewnienia właściwego projektowania i wdrożenia mechanizmów zabezpieczeń w ramach cyklu życia systemów informacyjnych

Źródło: opracowanie własne.

W etapie trzecim wyznaczono procesy funkcjonujące w ramach 7 wcześniej zdefiniowanych obszarów. Z uwagi na ramy objętościowe artykułu wymieniono jedynie procesy występujące w ramach obszaru I „Zarządzanie aktywami". Jak wskazują wyniki przeprowadzonych badań, w obszarze I wyłoniono 3 następujące procesy:

Proces 1: Odpowiedzialność za aktywa: inwentaryzacja aktywów, własność aktywów, akceptowalne użycie aktywów, zwrot aktywów.

Proces 2: Klasyfikacje informacji: klasyfikowanie informacji, oznaczenie informacji, postępowanie z aktywami.

Proces 3: Postępowanie z nośnikami: zarządzanie nośnikami wymiennymi, wycofanie nośników, przekazanie nośników.

W etapie piątym określono kryteria i wagi dla poszczególnych obszarów audytu, które odzwierciedlały ocenę audytora w zakresie zgodności danej sfery z obowiązującymi przepisami prawa, regulacjami wewnętrznymi oraz adekwatność przyjętych rozwiązań w stosunku do rodzaju audytowanej jednostki. Przypisane wagi zaprezentowano poniżej:

Obszar I: Zarządzanie aktywami – **16 pkt**,

Obszar II: Kontrola dostępu – **14 pkt**,

Obszar III: Kryptografia – **14 pkt**,
Obszar IV: Bezpieczeństwo fizyczne i środowiskowe – **14 pkt**,
Obszar V: Bezpieczna eksploatacja – **14 pkt**,
Obszar VI: Bezpieczeństwo komunikacji – **14 pkt**,
Obszar VII: Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych – **14 pkt**.

Przeprowadzenie testów i udokumentowanie prac audytowych było ostatnim etapem audytu bezpieczeństwa systemów informatycznych w podmiocie badań. Testy przeprowadzono przy użyciu listy kontrolnej oraz kwestionariusza kontroli wewnętrznej. W wyniku przeprowadzonego audytu dokonano następujących ustaleń[1] (tab. 2):

Tabela 2

Wyniki audytu bezpieczeństwa systemów informatycznych w obszarze I „Zarządzanie aktywami" w badanej jednostce

Nazwa i nr procesu	Treść ustaleń
1	2
Proces I: Odpowiedzialność za aktywa: – inwentaryzacja aktywów, – własność aktywów, – akceptowalne użycie aktywów, – zwrot aktywów.	1. Użytkownicy podpisali odpowiednie dokumenty potwierdzające przyjęcie aktywów na stan. 2. Aktywa są w odpowiedni sposób zabezpieczone przed kradzieżą, zniszczeniem oraz fizycznym uszkodzeniem. 3. Użytkownicy nie zostali odpowiednio przeszkoleni w zakresie ochrony informacji znajdujących się na aktywach wynoszonych poza jednostkę. 4. Użytkownicy nie są świadomi odpowiedzialności za naruszenie zasad ochrony znajdujących się na nich informacji. 5. W przypadku procesu inwentaryzacji aktywów audytor potwierdził, iż zakupione aktywa i oprogramowanie są ewidencjonowane według określonych kryteriów, a także przeprowadzana jest raz w roku inwentaryzacja sprzętu. 6. W jednostce nie prowadzi się ewidencji darmowego oprogramowania. 7. W procesie własności aktywów potwierdzono przypisanie aktywów konkretnym pracownikom. Tym samym obowiązki związane z bezpieczeństwem informacji przypisano właścicielom aktywów. 8. W procesie „akceptowalne użycie aktywów" wskazano, iż jednostka posiada odpowiednie procedury i uregulowania w zakresie zasad używania informacji i aktywów, działań, jakie należy podjąć w przypadku ich zużycia, zniszczenia lub kradzieży. 9. Brak jest procedury, która wymusza konieczność brania pod uwagę aspektu bezpieczeństwa w przypadku zakupu systemu informatycznego. 10. Zwrot aktywów jest odpowiednio dokumentowany, a pracownicy w przypadku rozwiązania stosunku pracy są rozliczani z posiadanych aktywów.
Proces 2: Klasyfikacje informacji: – klasyfikowanie informacji, – oznaczenie informacji, – postępowanie z aktywami.	1. Informacje w jednostce zostały sklasyfikowane w odpowiedni sposób, zgodnie z obowiązującymi w tym zakresie przepisami. 2. W audytowanym podmiocie przypisano właściwe uprawnienia do odpowiednich osób. 3. W podmiocie istnieje procedura w zakresie oznaczania informacji oraz postępowania z aktywami zgodnie z przyjętym schematem klasyfikacji.

[1] Z uwagi na ramy objętościowe opracowania przedstawiono ustalenia odnoszące się tylko do obszaru I.

1	2
Proces 3: Postępowanie z nośnikami: – zarządzanie nośnikami wymiennymi, – wycofanie nośników, – przekazanie nośników.	1. W jednostce istnieją właściwe procedury zarządzania nośnikami wymiennymi. 2. W procedurach wycofania nośników wymiennych określone zostały zasady kwalifikowania nośników do wycofania. 3. Prowadzona jest ewidencja nośników wycofanych, jednak nie są one w żaden sposób zabezpieczone. 4. W jednostce istnieją procedury wydawania nośników fizycznych. 5. Nośniki zawierające krytyczne dane są zabezpieczane przed nieautoryzowanym dostępem i modyfikacją.

Źródło: opracowanie własne.

Uwagi końcowe

Audyt bezpieczeństwa informatycznego w badanej jednostce sektora rządowego przeprowadzony został zgodnie z wytycznymi zdefiniowanymi w Załączniku A (punkt A.8–A.14) Polskiej Normy PN ISO/IEC 27001:2014-12. Audytorzy wyodrębnili 7 obszarów audytu oraz zidentyfikowali procesy wpływające na bezpieczeństwo informatyczne jednostki. Następnie, wykorzystując arkusze oceny i kwestionariusze na próbie wybranych użytkowników, przeprowadzili testy, które stanowiły podstawę oceny. Dzięki przeprowadzonemu audytowi w przedmiotowym zakresie udało się zidentyfikować słabości funkcjonowania systemu bezpieczeństwa informatycznego w badanej jednostce. Wyniki audytu były przesłanką dla kierownictwa organizacji audytowanej do wprowadzenia odpowiednich procedur i nowych mechanizmów ochrony danych. Ustalenia audytu potwierdziły, iż za bezpieczeństwo systemów informatycznych w znacznym stopniu odpowiadają ludzie, co implikuje konieczność podnoszenia świadomości pracowników w zakresie zagrożeń informatycznych oraz odpowiedzialności w przypadku utraty danych przez jednostkę.

Literatura

Board Briefing on IT Governance (2003). U.S.: IT Governance Institute.

Gałach, A. (2005). *Zarządzanie bezpieczeństwem systemu informatycznego – uniwersalna lista kontrolna*. Gdańsk: ODDK.

Liderman, K. (2012). *Bezpieczeństwo informacyjne*. Warszawa: PWN.

Łuczak, J. (2004). *Zarządzanie bezpieczeństwem informacji*. Poznań: Oficyna Współczesna.

Molski M., Łacheta, M. (2007). *Przewodnik audytora systemów informatycznych*. Gliwice: Helion.

Nowak, A., Scheffs, W. (2010). *Zarządzanie bezpieczeństwem informacyjnym*. Warszawa: AON.

Polski Komitet Normalizacyjny (2007). *Polska Norma PN-ISO/IEC 27001:2007. Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*. Warszawa.

Polski Komitet Normalizacyjny (2014). *Polska Norma PN-ISO/IEC 27001:2014-12. Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*. Warszawa.

Rozporządzenie Rady Ministrów z 12.04.2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Dz.U. poz. 526.

Ustawa z 27.08.2009 o finansach publicznych. Dz.U. 2013, poz. 885, z późn. zm.

Wspólne stanowisko Departamentu Informatyzacji Ministerstwa Administracji i Cyfryzacji i Departamentu Audytu Sektora Finansów Publicznych Ministerstwa Finansów odnośnie zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji. Ministerstwo Finansów. Pobrane z: http://www.mf.gov.pl/ministerstwo-finansow/dzialalnosc/finanse-publiczne/kontrola-zarzadcza-i-audyt-wewnetrzny/audyt-wewnetrzny--w-sektorze-publicznym/metodyka (20.05.2016).

Wytyczne dotyczące prowadzenia audytu bezpieczeństwa informacji przez komórkę audytu wewnętrznego. Ministerstwo Finansów. Pobrane z: http://www.mf.gov.pl/ministerstwo-finansow/dzialalnosc/finanse--publiczne/kontrola-zarzadcza-i-audyt-wewnetrzny/audyt-wewnetrzny-w-sektorze-publicznym/metodyka (20.05.2016).

Żebrowski, A., Kwiatkowski, W. (2000). *Bezpieczeństwo informacji III Rzeczypospolitej*. Kraków: Abrys.

THE ROLE AND THE TASKS OF IT SECURITY AUDIT ON THE EXAMPLE OF THE GOVERNMENT SECTOR UNIT

Abstract: *Purpose* – The aim of this article is to present the role and the tasks of IT security audit in public finance sector units as well as to show threats of its functioning.
Design/methodology/approach – The methods used to attain the objective included the analysis of literature and legislation concerning the subject. The empirical part of the article presents a case study of the IT security audit carried out in government sector unit. Conclusions were based on induction method.
Findings – The article presents theoretical aspect of IT security audit as well as practical approach to this subject.
Originality/value – The authors analyzed the tasks of the IT system audit and identified threats of functioning of this system.

Keywords: internal audit, IT security system audit, IT audit, governments sector units

Cytowanie
Bartoszewicz, S., Bartoszewicz, A. (2016). Rola i zadania audytu bezpieczeństwa systemów informatycznych na przykładzie jednostki sektora administracji rządowej. *Finanse, Rynki Finansowe, Ubezpieczenia*, *6/1* (84), 269–279. DOI: 10.18276/frfu.2016.84/1-23.